最新セキュリティマネジメント（第4回）

セキュリティリスク管理体制の構築

2021.09.21

経済産業省が策定した「セキュリティ経営ガイドライン」で、経営者が社内に指示すべきポイントとして示された「重要10項目」。今回は2番目の項目となる「サイバーセキュリティリスク管理体制の構築」について解説する。

管理体制構築の進め方

経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定した「サイバーセキュリティ経営ガイドライン Ver2.0」は、企業のIT活用を推進する上で経営者が認識すべきサイバーセキュリティに関する原則や、経営者がリーダーシップを持って取り組むべき項目をまとめたものである。

本ガイドラインでは、経営者が認識すべき3原則として以下の3つを挙げている。

・サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めること
・ビジネスパートナーや委託先も含めたサプライチェーンに対する対策が必要
・サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

ただ、多忙を極める経営者がセキュリティ対策を単独で行うことは難しい。そこで上記の原則に基づき、セキュリティ対策の実務を担当するCISO（最高情報セキュリティ責任者）などの幹部に指示を出すことになる。前回は指示すべきポイントとなる「重要10項目」の最初に挙げられた項目「サイバーセキュリティリスクの認識、組織全体での対応方針の策定」を紹介した。今回は2番目の項目「サイバーセキュリティリスク管理体制の構築」について、次回（第5回）は「人材確保」にスポットを当てて解説する。

すべての部署が「当事者」に

管理体制の構築と聞いて、「うちの会社は情シス（情報システム部）がしっかり担当しているから安心」と考えてしまう経営者は少なくない。これは、ITに精通したスタッフで構成された情シスへの信頼度が高いことに加え、日本企業がITに関する業務を情シスや外部ベンダーに任せるケースが多いことも理由と思われる。しかし、本ガイドラインではサイバーセキュリティリスク管理を「企業全体で取り組むべきもの」として捉え、情シス以外の部署も当事者として関わる必要性を示している。具体的には管理部門のリスクマネジメント関連部署、工場・店舗などの各事業部門、経営企画部門など社内の多くの部署が含まれる。

企業が製品・サービスを展開する際には、企画から提供に至る各段階でサイバーセキュリティ対策を講じる必要がある。また、サプライチェーン全体を考えた場合は海外拠点、グループ会社、取引先など、組織を超えた対策が重要だ。さらに、インシデント発生時には法務、広報とも連携した対応が求められる。つまり、セキュリティ対策は企業全体で取り組むものであり、「まったく無関係の部署は存在しない」という表現も過言ではないだろう。

「セキュリティ統括機能」の役割… 続きを読む